

---

# 1 Kantara Initiative eGovernment 2 Implementation Profile of SAML V2.0

## 3 Version 2.0

4 **Working Draft 02**  
5 **March 10, 2010**

6 **Document identifier:**  
7 draft-kantara-egov-saml2-profile-2.0

8 **Location:**  
9 TBD

10 **Editors:**  
11 Scott Cantor, Internet2

12 **Contributors:**  
13 Kantara eGovernment WG  
14 Andreas Åkre Solberg, UNINETT

15 **Abstract:**  
16 This document contains an implementation profile for eGovernment use of SAML V2.0, suitable  
17 for the purposes of testing conformance of implementations of SAML V2.0. It is not a deployment  
18 profile, and does not provide for or reflect specific behavior expected of implementations when  
19 used within a particular deployment context.

20 **Notice:**  
21 This document has been prepared by Participants of Kantara Initiative. Permission is hereby  
22 granted to use the document solely for the purpose of implementing the Specification. No rights  
23 are granted to prepare derivative works of this Specification. Entities seeking permission to  
24 reproduce portions of this document for other uses must contact Kantara Initiative to determine  
25 whether an appropriate license for such use is available.

26 Implementation or use of certain elements of this document may require licenses under third party  
27 intellectual property rights, including without limitation, patent rights. The Participants of and any  
28 other contributors to the Specification are not and shall not be held responsible in any manner for  
29 identifying or failing to identify any or all such third party intellectual property rights. This  
30 Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of  
31 any kind, expressed or implied, including any implied warranties of merchantability, non-  
32 infringement of third party intellectual property rights, and fitness for a particular purpose.  
33 Implementers of this Specification are advised to review Kantara Initiative's website  
34 (<http://www.kantarainitiative.org/>) for information concerning any Necessary Claims Disclosure  
35 Notices that have been received by the Kantara Initiative Board of Trustees.

36  
37 Copyright: The content of this document is copyright of Kantara Initiative. © 2010 Kantara  
38 Initiative.  
39

40 **Table of Contents**

41	1 Introduction.....	3
42	1.1 Notation.....	3
43	1.2 Normative References.....	4
44	2 SAML V2.0 Implementation Profile.....	5
45	2.1 Required Information.....	5
46	2.2 Metadata and Trust Management.....	5
47	2.2.1 Conformance Criteria.....	6
48	2.3 Name Identifiers.....	6
49	2.3.1 Conformance Criteria.....	6
50	2.4 Attributes.....	6
51	2.4.1 Conformance Criteria.....	6
52	2.5 Single Sign-On.....	6
53	2.5.1 Identity Provider Discovery.....	7
54	2.5.1.1 Conformance Criteria.....	7
55	2.5.2 Authentication Requests.....	7
56	2.5.2.1 Binding and Security Requirements.....	7
57	2.5.2.1.1 Conformance Criteria.....	7
58	2.5.2.2 Message Content.....	7
59	2.5.2.2.1 Conformance Criteria.....	7
60	2.5.3 Responses.....	8
61	2.5.3.1 Binding and Security Requirements.....	8
62	2.5.3.1.1 Conformance Criteria.....	8
63	2.5.3.2 Message Content.....	8
64	2.5.3.2.1 Conformance Criteria.....	8
65	2.6 Artifact Resolution.....	8
66	2.6.1 Artifact Resolution Requests.....	9
67	2.6.1.1 Conformance Criteria.....	9
68	2.6.2 Artifact Resolution Responses.....	9
69	2.6.2.1 Conformance Criteria.....	9
70	2.7 Single Logout.....	9
71	2.7.1 Logout Requests.....	9
72	2.7.1.1 Binding and Security Requirements.....	9
73	2.7.1.1.1 Conformance Criteria.....	9
74	2.7.1.2 User Interface Behavior.....	10
75	2.7.1.2.1 Conformance Criteria.....	10
76	2.7.2 Logout Responses.....	10
77	2.7.2.1 Binding and Security Requirements.....	10
78	2.7.2.1.1 Conformance Criteria.....	10
79	Appendix A. Open Issues.....	11
80		

---

# 81 1 Introduction

82 SAML V2.0 is a rich and extensible standard that must be profiled to be used interoperably, and the  
83 profiles that typically emerge from the broader standardization process usually remain fairly broad and  
84 include a number of options and features that increase the burden for implementers and make  
85 deployment-time decisions more difficult.

86 The Kantara Initiative eGovernment Implementation Profile provides a SAML V2.0 conformance  
87 specification for Identity Provider and Service Provider implementations operating in eGovernment  
88 federations and deployments. The profile is based on the SAML V2.0 specifications created by the  
89 Security Services Technical Committee (SSTC) of OASIS, and related specifications approved by that  
90 body. It constrains and supplements the base SAML V2.0 features, elements, and attributes required for  
91 eGovernment federations and deployments.

92 Implementation profiles define the features that software implementations must support such that  
93 deployers can be assured of the ability to meet their own (possibly varied) deployment requirements.  
94 Deployment profiles define specific options and constraints to which deployments are required to conform;  
95 they guide product configuration and federation operations, and provide criteria against which actual  
96 deployments may be tested. This document does not include a deployment profile, but reflects the  
97 features deemed necessary or desirable from software implementations in support of a variety of  
98 deployment profiles planned and in use. This includes requirements deemed useful to further the eventual  
99 goal of interfederation between deployments.

## 100 1.1 Notation

101 This specification uses normative text to describe the use of SAML capabilities.

102 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD  
103 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as  
104 described in [RFC2119]:

105       ...they MUST only be used where it is actually required for interoperation or to limit behavior  
106       which has potential for causing harm (e.g., limiting retransmissions)...

107 These keywords are thus capitalized when used to unambiguously specify requirements over protocol and  
108 application features and behavior that affect the interoperability and security of implementations. When  
109 these words are not capitalized, they are meant in their natural-language sense.

110       Listings of XML schemas appear like this.

111       Example code listings appear like this.

113 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for  
114 their respective namespaces as follows, whether or not a namespace declaration is present in the  
115 example:

- 116     • The prefix `saml2:` stands for the SAML 2.0 assertion namespace,  
117       `urn:oasis:names:tc:SAML:2.0:assertion`
- 118     • The prefix `saml2p:` stands for the SAML 2.0 protocol namespace,  
119       `urn:oasis:names:tc:SAML:2.0:protocol`
- 120     • The prefix `md:` stands for the SAML 2.0 metadata namespace,  
121       `urn:oasis:names:tc:SAML:2.0:metadata`
- 122     • The prefix `idpdisc:` stands for the Identity Provider Discovery Service Protocol and Profile  
123       [IdPDisco] namespace, `urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-`  
124       `protocol`

125 • The prefix `mdattr:` stands for the Metadata Extension for Entity Attributes Version 1.0 [MetaAttr]  
126 namespace, `urn:oasis:names:tc:SAML:metadata:attribute`

127 This specification uses the following typographical conventions in text: `<ns:Element>`, Attribute,  
128 **Datatype**, OtherCode.

## 129 1.2 Normative References

130	[RFC2119]	IETF RFC 2119, <i>Key words for use in RFCs to Indicate Requirement Levels</i> , 131 March 1997. <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
132	[RFC2616]	IETF RFC 2616, <i>Hypertext Transfer Protocol – HTTP/1.1</i> , June 1999. <a href="http://www.ietf.org/rfc/rfc2616.txt">http://www.ietf.org/rfc/rfc2616.txt</a>
134	[RFC2818]	IETF RFC 2818, <i>HTTP Over TLS</i> , May 2000. <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a>
135	[IdPDisco]	OASIS Committee Specification, <i>Identity Provider Discovery Service Protocol and Profile</i> , March 2008. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf</a>
138	[MetaAttr]	OASIS Committee Specification, <i>SAML V2.0 Metadata Extension for Entity Attributes Version 1.0</i> , August 2009. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf</a>
141	[MetaIOP]	OASIS Committee Specification, <i>SAML V2.0 Metadata Interoperability Profile Version 1.0</i> , August 2009. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf</a>
144	[SAML2Core]	OASIS Standard, <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf</a>
147	[SAML2Meta]	OASIS Standard, <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a>
150	[SAML2Bind]	OASIS Standard, <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf</a>
153	[SAML2Prof]	OASIS Standard, <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf</a>
156	[SAML2Err]	OASIS Approved Errata, <i>SAML V2.0 Errata</i> . <a href="http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf">http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf</a>
158	[SAML-X500]	OASIS Committee Specification, <i>SAML V2.0 X.500/LDAP Attribute Profile</i> , March 159 2008. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf</a>
160		

## 161 Non-Normative References

162	[eGov15]	Kyle Meadors, <i>Liberty Alliance eGov Profile for SAML 2.0 Version 1.5</i> .
-----	----------	---

---

## 163 2 SAML V2.0 Implementation Profile

164 This profile specifies behavior and options that implementations of a selected set of SAML V2.0 profiles  
165 [SAML2Prof] are required to support. The requirements specified are *in addition to* all normative  
166 requirements of the original profiles, as modified by the Approved Errata [SAML2Err], and readers should  
167 be familiar with all relevant reference documents. Any such requirements are not repeated here except  
168 where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in  
169 errata, but remain implied.

170 SAML leaves substantial latitude to implementations with regard to how software is architected and  
171 combined with authentication and application infrastructure. Where the terms "Identity Provider" and  
172 "Service Provider" are used, they should be understood to include the total software footprint intended to  
173 provided the desired functionality; no specific assumptions are made as to how the required features are  
174 exposed to deployers, only that there is some method for doing so.

### 175 2.1 Required Information

176 **Identification:** TBD

177 **Contact information:** TBD

178 **Description:** Given below

179 **Updates:** Liberty Alliance eGov Profile for SAML 2.0 [eGov15]

### 180 2.2 Metadata and Trust Management

181 Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of  
182 SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 profiles referenced  
183 by subsequent sections. Additional expectations around the use of particular metadata elements related to  
184 profile behavior may be encountered in those sections.

185 Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetalOP].

186 Implementations MUST support the **TBD: insert profile for PKI here**

187 It is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but  
188 implementations MUST support the following mechanisms for the importation of metadata:

- 189     • local file  
190     • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL  
191        [RFC2818]

192 In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache  
193 management; other cache control support is OPTIONAL. Implementations SHOULD support the use of  
194 more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a  
195 single entity's metadata is present in more than one source.

196 In accordance with [MetalOP], importation of multiple entities' metadata contained within an  
197 <md:EntitiesDescriptor> element MUST be supported.

198 Verification of metadata, if supported, MUST include XML signature verification at least at the root  
199 element level, and SHOULD support the following mechanisms for signature key trust establishment:

- 200     • direct comparison against known keys  
201     • some form of path-based certificate validation against one or more trusted root certificates and  
202        certificate revocation lists

203 The latter mechanism does not impose a particular profile for certificate validation, as no such profile has  
204 wide enough adoption across tools and libraries to warrant such a requirement, but should be understood  
205 as being consistent with the "usual" practices encountered in the implementation of certificate validation.  
206 Where possible, implementations SHOULD document known limitations of the mechanisms they employ.

207 Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0  
208 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension  
209 mechanism.

210 Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without  
211 significant disruption of services.

## 212 **2.2.1 Conformance Criteria**

213 TBD

## 214 **2.3 Name Identifiers**

215 In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity  
216 Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier  
217 formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- 218     • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent  
219     • urn:oasis:names:tc:SAML:2.0:nameid-format:transient

220 Support for other formats is OPTIONAL.

## 221 **2.3.1 Conformance Criteria**

222 TBD

## 223 **2.4 Attributes**

224 In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity  
225 Provider and Service Provider implementations MUST support the generation and consumption of  
226 <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-  
227 X500].

228 The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g.,  
229 <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an  
230 alternative.

## 231 **2.4.1 Conformance Criteria**

232 TBD

## 233 **2.5 Single Sign-On**

234 This section defines an implementation profile of the SAML V2.0 Web Browser SSO profile [SAML2Prof].

235 **2.5.1 Identity Provider Discovery**

236 Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery  
237 Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

238 **2.5.1.1 Conformance Criteria**

239 TBD

240 **2.5.2 Authentication Requests**

241 **2.5.2.1 Binding and Security Requirements**

242 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect  
243 binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the  
244 generation or verification of signatures in conjunction with this binding.

245 Support for other bindings is OPTIONAL.

246 **2.5.2.1.1 Conformance Criteria**

247 TBD

248 **2.5.2.2 Message Content**

249 In addition to standard core- and profile-driven requirements, Service Provider implementations MUST  
250 support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes  
251 (when appropriate):

- 252 • AssertionConsumerServiceURL
- 253 • ProtocolBinding
- 254 • ForceAuthn
- 255 • IsPassive
- 256 • AttributeConsumingServiceIndex
- 257 • <saml2p:RequestedAuthnContext>
- 258 • <saml2p:NameIDPolicy>

259 Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and  
260 attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate  
261 errors when confronted by particular request options. However, implementations MUST fully support the  
262 options enumerated above.

263 Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the  
264 value "exact" for the Comparison attribute.

265 **2.5.2.2.1 Conformance Criteria**

266 TBD

267 **2.5.3 Responses**

268 **2.5.3.1 Binding and Security Requirements**

269 Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST and  
270 HTTP-Artifact bindings [SAML2Bind] for the transmission of <saml2p:Response> messages.

271 Support for other bindings, and for artifact types other than  
272 urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL.

273 Identity Providers and Service Providers MUST support the generation and consumption of unsolicited  
274 <saml2p:Response> messages (i.e., responses that are not the result of a <saml2p:AuthnRequest>  
275 message).

276 Identity Provider and Service Provider implementations MUST support the signing of  
277 <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element  
278 is OPTIONAL.

279 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the  
280 <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the  
281 <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL.

282 **2.5.3.1.1 Conformance Criteria**

283 TBD

284 **2.5.3.2 Message Content**

285 The Web Browser SSO Profile allows responses to contain any number of assertions and statements.  
286 Identity Provider implementations MUST allow the number of <saml2:Assertion>,  
287 <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the  
288 <saml2p:Response> message to be limited to one.

289 In turn, Service Provider implementations MAY limit support to a single instance of those elements when  
290 processing <saml2p:Response> messages.

291 Identity Provider implementations MUST support the inclusion of a Consent attribute in  
292 <saml2p:Response> messages, and a SessionIndex attribute in <saml2:AuthnStatement>  
293 elements.

294 Service Provider implementations that provide some form of session semantics MUST support the  
295 <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute.

296 **2.5.3.2.1 Conformance Criteria**

297 TBD

298 **2.6 Artifact Resolution**

299 This section defines an implementation profile of the SAML V2.0 Artifact Resolution profile [SAML2Prof].

300 **2.6.1 Artifact Resolution Requests**

301 Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP binding  
302 [SAML2Bind], using HTTP as a transport, for the transmission of <saml2p:ArtifactResolve>  
303 messages.

304 Implementations MUST support the use of SAML message signatures to authenticate requests; support  
305 for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is  
306 OPTIONAL.

307 **2.6.1.1 Conformance Criteria**

308 TBD

309 **2.6.2 Artifact Resolution Responses**

310 Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP binding  
311 [SAML2Bind], using HTTP as a transport, for the transmission of <saml2p:ArtifactResponse>  
312 messages.

313 Implementations MUST support the use of SAML message signatures to authenticate requests; support  
314 for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is  
315 OPTIONAL.

316 **2.6.2.1 Conformance Criteria**

317 TBD

318 **2.7 Single Logout**

319 This section defines an implementation profile of the SAML V2.0 Single Logout profile [SAML2Prof].

320 **2.7.1 Logout Requests**

321 **2.7.1.1 Binding and Security Requirements**

322 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect and  
323 SAML SOAP (using HTTP as a transport) bindings [SAML2Bind] for the transmission of  
324 <saml2p:LogoutRequest> messages, including the generation or verification of message signatures in  
325 conjunction with both bindings. Support for TLS or other transport-based authentication in conjunction with  
326 the SAML SOAP binding is OPTIONAL.

327 Support for other bindings is OPTIONAL.

328 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the  
329 <saml2:EncryptedID> element when using the HTTP-Redirect binding.

330 **2.7.1.1.1 Conformance Criteria**

331 TBD

332 **2.7.1.2 User Interface Behavior**

333 Identity Provider and Service Provider implementations MUST support "local" logout as well as initiation of  
334 Single Logout, subject to deployer and user option.

335 **2.7.1.2.1 Conformance Criteria**

336 TBD

337 **2.7.2 Logout Responses**

338 **2.7.2.1 Binding and Security Requirements**

339 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect and  
340 SAML SOAP (using HTTP as a transport) bindings [SAML2Bind] for the transmission of  
341 <saml2p:LogoutResponse> messages, including the generation or verification of message signatures  
342 in conjunction with both bindings. Support for TLS or other transport-based authentication in conjunction  
343 with the SAML SOAP binding is OPTIONAL.

344 Support for other bindings is OPTIONAL.

345 **2.7.2.1.1 Conformance Criteria**

346 TBD

## Appendix A. Open Issues

- 348     • Need an alternative to IOP, or agreement to drop PKI outside of metadata exchange. Alternative  
349       needs to specify PKI to some degree AND address the exact content and semantics of metadata  
350       as relates to runtime certificate evaluation and/or identity of SAML peer.
- 351     • Security features required in support of SOAP binding?
- 352     • Do implementations need to be able to prevent non-use of TLS on front-channel?
- 353     • Need for more than exact AuthnContext matching?
- 354     • Need for specific MTI behavior on ACS checking?
- 355     • Need some clarification of some of the original single logout language around user consent.
- 356     • Updated crypto algorithm conformance rules for implementers and deployers?
- 357     • Populate with conformance criteria.
- 358     • Is feature discussion of AuthnContext and metadata tagging enough to cover LOA issues?

---

## 359      **Appendix B. Change Log**

- 360      • Draft 01: first working draft based on similar document created by InCommon federation  
361      • Draft 02: first round of feedback incorporated, deployment section dropped, new section on  
362        Artifact Resolution added, artifact added for SSO responses, SOAP added for logout, discovery  
363        moved under SSO, language on non-string attributes added, changed SHOULD to MUST for IdP  
364        support of selected AuthnRequest features